USAID
FROM THE AMERICAN PEOPLE

USAID CYBERSECURITY FOR CRITICAL INFRASTRUCTURE IN UKRAINE ACTIVITY

CYBERSECURITY PRODUCTS AND SERVICES RAPID MARKET ASSESSMENT

Program Title:	USAID Cybersecurity for Critical Infrastructure in Ukraine
Sponsoring USAID Office:	USAID/Ukraine
Contract Number:	72012120C00002
Contractor:	DAI Global, LLC
Submission Date:	April 7, 2021, re-submitted June 4, 2021
Author:	DAI Global, LLC and SocialBoost

TABLE OF CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

LIST OF ABBREVIATIONS

CCI	Center for Cybersecurity Innovation
CEO	Chief Executive Officer
CI	Critical Infrastructure
CICIPA	Critical Infrastructure Cybersecurity Incident Preparedness Assessment
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMM	Cybersecurity Maturity Model
CTO	Chief Technology Officer
DDoS	Distributed Denial of Service
DLP	Data Leakage Protection
EU	European Union
GDP	Gross Domestic Product
GOU	Government of Ukraine
ICT	Information and Communications Technology
IT	Information Technology
KII	Key Informant Interview
LSEC	Leaders in Security
MDR	Managed Detection and Response
NBU	National Bank of Ukraine
NIST	United States National Institute of Standards and Technology
NSDC	National Security and Defense Council of Ukraine
OT	Operations Technology
P&L	Profit and Loss
Pentest	Penetration Testing
PwC	PricewaterhouseCoopers
QA	Quality Assurance

R&D	Research and Development
SMB	Small and Medium-sized Businesses
SOC	Security Operations Center
SOE	State-owned Enterprise
SSL	Secure Sockets Layer
TISM	Threat Intelligence Sharing Mechanism
TLS	Transport Layer Security
UAH	Ukrainian hryvnia
USF	Ukrainian Startup Fund
USAID	United States Agency for International Development
USD	United States Dollar
UTM	Unified Threat Management
VPN	Virtual Private Network

EXECUTIVE SUMMARY

Ukraine's cybersecurity market is underdeveloped when compared to the markets of other European economies. According to 2019 estimates, the size is less than a tenth of one percent of the country's USD 153.78 billion[1] gross domestic product (GDP). According to a study of the 2016 European Union (EU) market,[2] the cybersecurity market represented on average 1.1% of a member state's GDP, meaning that Ukraine's cybersecurity market size would need to balloon to USD 1.69 billion to measure up to the EU average.

This shortfall in cybersecurity spending reflects Ukraine's primary cybersecurity market challenge: unaddressed (and often unrecognized) need for cybersecurity services. The USAID Cybersecurity for Critical Infrastructure in Ukraine Activity (the Activity) aims to bolster demand for cybersecurity services and support cybersecurity providers in meeting that demand. These demand- and supply-side interventions will help address Ukraine's cybersecurity challenges and contribute to increasing the market size relative to GDP.

This Rapid Market Assessment (RMA) was designed to assess the current market for cybersecurity products and services in Ukraine and highlight market challenges, risks, and opportunities for targeted assistance and investment. Through a review of open-source data, surveys of cybersecurity customers and providers, and key informant interviews (KIIs) with representatives from major cybersecurity players, the Activity found that there are significant obstacles for growth in the current cybersecurity market in Ukraine, but also great opportunities. Due to a weak regulatory environment and lack of awareness about cybersecurity threats and the potential cost of an incident, demand for cybersecurity services is relatively low. This low demand—coupled with lack of qualified cybersecurity professionals and limited access to capital—has constrained the nascent cybersecurity sector, and small and medium-sized businesses (SMBs) most acutely.

The positive news is that significant potential exists to promote cybersecurity investments in public and private sector entities and leverage the country's significant technical and business services resources to create a thriving cybersecurity market.

INTRODUCTION

The goal of the Activity is to reduce cybersecurity vulnerabilities in critical infrastructure (CI) and transform Ukraine from a compromised, reactive cybersecurity actor to a proactive cybersecurity leader. To achieve this goal, the Activity will pursue the following strategic objectives:

Strategic Objective 1: Create a safe and trusted environment to accelerate the development of people, processes, and technology in support of cybersecurity across CI sectors and assets in Ukraine.

Strategic Objective 2: Strengthen Ukraine as a sovereign nation built on a secure, protected, and dynamic economy, supported by a talented pool of human capital.

Strategic Objective 3: Stimulate demand for and supply of Ukrainian cybersecurity solutions and service providers to empower, equip, and finance cybersecurity entrepreneurs and businesses.

---

[1] The World Bank, "GDP (Current US$) – Ukraine," Accessed March 15, 2021, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=UA.

[2] European Commission, *Cybersecurity Industry Market Analysis – CIMA (*Luxembourg: Publications Office of the European Union), p. 84.

In support of Strategic Objective 3, the Activity assessed the cybersecurity market in Ukraine. The RMA was designed to assess the current market for cybersecurity products and services in Ukraine and highlight market challenges, risks, and opportunities for targeted assistance and investment. It reflects the critical importance of the private sector in cybersecurity, drawing on successful models from the U.S., where the public and private sectors work together closely, and Israel, where public sector policy (and funding) directly supports innovation in and growth of the cyber sector.

METHODOLOGY

The RMA draws on information from multiple sources, including open-source data and interviews of key cybersecurity stakeholders. Open-source data included the websites of cybersecurity providers, LinkedIn profiles, profiles on the IT industry, the website dou.ua, articles about companies including information about clients and location, market studies, financial reports, and paid services such as YouControl. In addition, the Activity conducted three types of interviews: 1) survey interviews of major cybersecurity consumers, 2) survey interviews of cybersecurity product and service providers, and 3) in-depth key informant interviews (KIIs) of cybersecurity providers to supplement the surveys. Each category of interview is described in more detail below and in Annex 1.

OPEN-SOURCE DATA

Reliable statistics on the cybersecurity market are limited, as are breakdowns of the sector. For example, no statistics are available on cybersecurity product imports, most consulting firm revenue, the share of value-added consulting services for product sellers, the share of hardware resale for cybersecurity consultants, the share of cybersecurity consulting at large consulting firms, the number of people employed in the sector as either third-party consultants or in-house cyber specialists, the total public sector spending on cybersecurity, or defense and security service spending on cybersecurity. Nor did public sector procurement data provide a detailed breakdown of products vs. services.

This lack of data made it difficult for the Activity to assess the cybersecurity market size and identify appropriate survey participants, resulting in a need for additional data. To correct for this issue, the research team conducted a series of KIIs to corroborate and supplement the open-source data and survey interviews. Between the survey interviews and KIIs, the interviews covered an estimated 24.4% of the providers of cybersecurity goods and services on the Ukrainian market and 43.4% of the providers of consulting services.

SURVEYS

Survey interviews with 23 consumers of cybersecurity goods and services

The research team selected 23 companies for survey interviews, based on an original list of 1,500 companies identified as customers on cybersecurity provider websites. After sorting these 1,500 companies by industry, the team identified the 10 industries with the highest number of companies: 1) government, 2) finance and banking, 3) manufacturing, 4) product development, 5) telecommunications, 6) healthcare, 7) energy, 8) outsourcing services, 9) retail, and 10) payment processing. The team then used publicly available information to rank the top 10 companies in each category by revenue and attempted to get three interviews in each category. Ultimately, the team conducted 23 interviews with firms across 10 categories.

Interviews and questionnaires of 22 providers of cybersecurity goods and services

The research team surveyed 22 cybersecurity firms, representing an estimated 31% of the total market. To select these 22 firms, the team used research databases and websites to identify 72 companies supplying cybersecurity products and consulting services. The team first categorized the companies as product or service providers, then by size (small – fewer than 25 employees, medium – 25-100 employees, or large – more than 100). The team aimed for an even distribution of companies across each segment, attempting to obtain interviews with one or two of the leading companies in each segment.

KEY INFORMANT INTERVIEWS

The research team interviewed 10 senior professionals in the Ukrainian cybersecurity market. These experts ranged from the directors of local branches of international cybersecurity firms to the founders of Ukrainian cybersecurity start-ups. Topics covered in these in-depth discussions included market conditions and challenges, as well as the potential for increasing the demand for cybersecurity products and services.[3]

KEY FINDINGS

CYBERSECURITY PRODUCTS AND SERVICES

OVERVIEW

According to the U.S. National Institute for Standards and Technology (NIST) Cyber Security Framework,[4] cybersecurity products and services address five key functions in countering cyberattacks: (1) Identify, (2) Protect, (3) Detect, (4) Respond and (5) Recover (see Table 1). Services in each of these functions can be performed by third-party consultants or in-house. It is important to note that "Identify," "Respond," and "Recover" are processes that primarily involve people. "Detection" is typically automated, though monitoring functions still require people. For cybersecurity, key informant interviewees consistently stressed that people and processes are key. Cybersecurity defense is typically preventative and reactive rather than innovative as cybersecurity professionals are constantly monitoring and playing catch-up as new threats arise. Interviewees told us that, in general, solutions are developed for concrete problems that confront CI operators; unfortunately, in cybersecurity, it is not in the solutions but the attacks that one finds the most rapid innovation.

[3] These interviews were extraordinarily valuable, and the Activity recommends continuing them, targeting the firms shown in the "GOU Public Tenders" section below. Future interviews would elicit valuable feedback and information that could inform the Activity's forthcoming Center for Cybersecurity Innovation (CCI) Plan and Investment Strategy.

[4] Nicole.keller@nist.gov. "An Introduction to the Components of the Framework." NIST, June 15, 2020. https://www.nist.gov/cyberframework/online-learning/components-framework.

TABLE 1: CYBERSECURITY PRODUCTS AND SERVICES

FUNCTION	PRODUCT	SERVICE
Identify	Vulnerability management scanners, penetration testing platforms, automated ISMS platforms, static code analyzers	Penetration testing, security audit and testing, compliance audit, supply chain risk audit, employee testing by social engineering
Protect	Hardware (Firewall), virtual private network (VPN), anti-virus, protective technology, encryption, certificates (transport layer security [TLS]/secure sockets layer [SSL]), distributed denial of service (DDoS) protection, cloud storage, personal identity protection	Compliance implementation; training; data leakage protection; access management; awareness and training; processes and procedures; planning for detection, response, and recovery; threats intelligence platform; maintenance procedures
Detect	Threat detection, security operations center (SOC) (in-house)	Continuous monitoring, Security Operations Center (SOC) (outsourced)
Respond	NA	Analysis, mitigation, improvements
Recover	Data Backup & Recovery technologies	Data recovery, improvements, forensics

MARKET STRUCTURE

In Ukraine, end-users acquire cybersecurity products either from product vendors (primarily through their resellers) or through consulting companies engaged to provide cybersecurity services. The products may be hardware or software. Product vendors may also offer limited value-added cybersecurity consulting services to end-users.

Consulting firms provide services with varying levels of sophistication. Some provide fairly unsophisticated services, some provide sophisticated but without reselling products (such as EY and Deloitte), and others offering sophisticated services who also resell products as part of a turnkey solution. These latter firms also offer the possibility of outsourcing functions to them, like SOC.

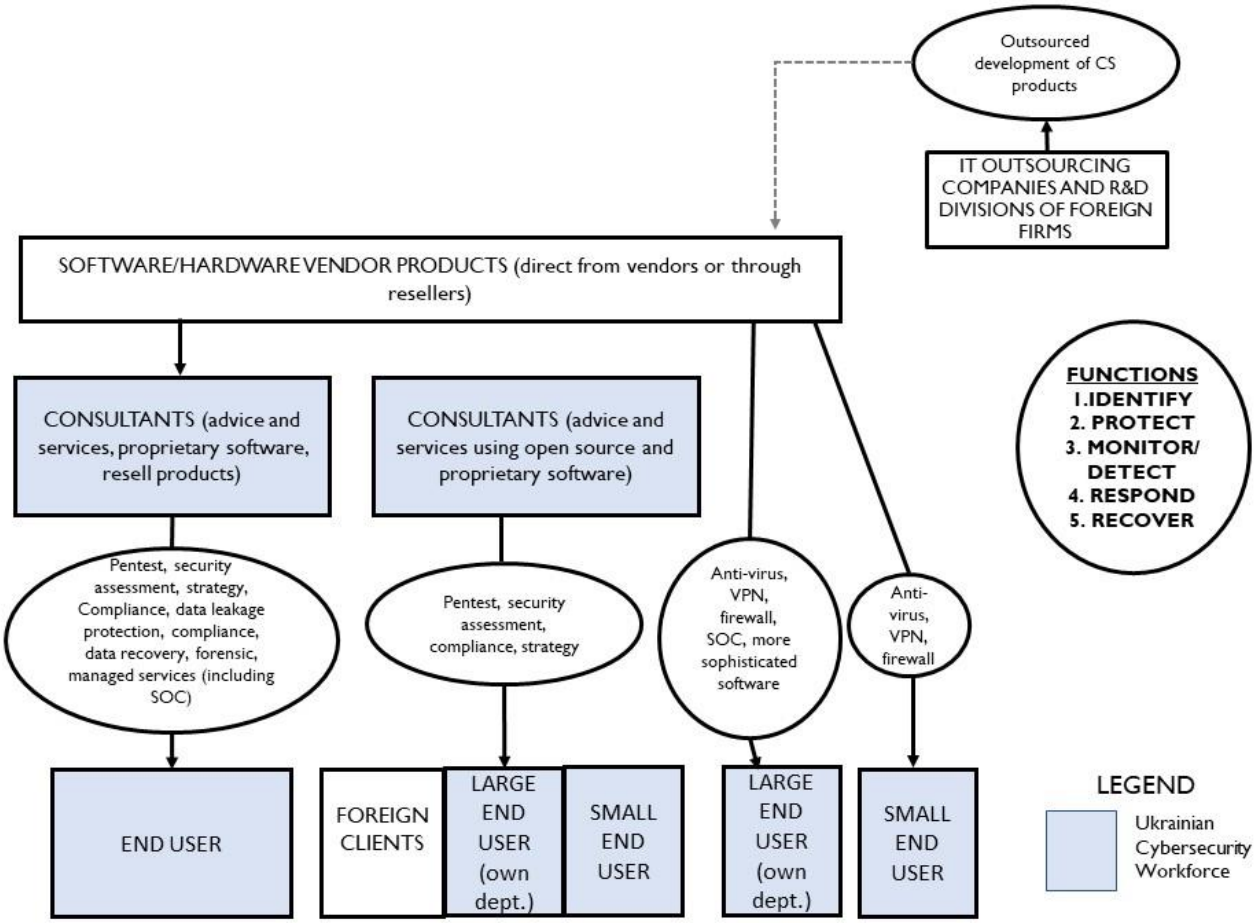
Interviews with consulting firms revealed that consulting services make up an estimated 15-30% of the Ukrainian market. To overcome a resistance in the market to paying for consulting services, consulting firms at times offset some of the costs of providing such services with margins on resold products.

Figure 1 describes the structure of the Ukrainian cybersecurity market. It's important to note that the IT outsourcing market depicted in the upper right-hand corner is not part of the Ukrainian cybersecurity market for products and services, but actually functions as a competitor for workforce talent in the market. Moreover, the cybersecurity services

> 20% ON TOP OF PRODUCT COSTS OUGHT TO GO TO CONSULTING TO ENSURE PRODUCTS ARE PROPERLY INSTALLED AND USED. OTHERWISE THEY WILL BECOME "SHELFWARE."
>
> - CONSULTING FIRM INTERVIEWEE

include both third-party consultants and the in-house staff of end-users, who perform much of the work required for effective cybersecurity. In addition to vendors and resellers, distributors manage channels and logistics. These distributors serve as the go-betweens for vendors, resellers, and end users. The cybersecurity workforce is shaded in blue in the diagram below.

FIGURE 1: UKRAINIAN CYBERSECURITY MARKET STRUCTURE



UKRAINIAN IT OUTSOURCING FIRMS ARE NOT A PART OF THE CYBERSECURITY MARKET AND ACTUALLY COMPETE FOR TALENT ON THE LABOR MARKET

Some Ukrainian IT outsourcing companies contribute to development of cybersecurity products by foreign clients and international markets. The large Ukrainian IT outsourcing firms do not create and market cybersecurity products of their own. The value of their outsourcing services on the Ukrainian cybersecurity market is reflected as a fraction of the total purchase price for the small amount of cybersecurity end products sold domestically. In fact, well-financed outsourcing companies compete with cybersecurity providers for specialist talent, which constrains workforce growth in the cybersecurity sector, especially for SMBs.

ANALYSIS OF CYBERSECURITY PRODUCTS AND SERVICES

FINDINGS FROM PROVIDERS OF CYBERSECURITY PRODUCTS AND SERVICES

Based on a thorough analysis of the market, the research team estimated that approximately 72 firms provide cybersecurity products and services in Ukraine. Survey respondents corroborated this number, with 91% estimating that there were fewer than 100 firms on the market.

Table 2 below shows the top vendors and consulting service providers grouped by size (i.e., by the number of employees, as defined earlier).[5]

TABLE 2: MAJOR PRODUCT AND SERVICE PROVIDERS (2019)

SEGMENT	SMALL	MEDIUM	LARGE
Products	Epos	Infozahyst	Softprom
	Infosafe IT	Svit IT	Cisco Systems
	OptiData	Author	Clario Tech / Zeo Alliance / Kromtech
	Atola Technology	Netwave LLC	Cipher
		Remme	
		Winncom Technologies	
Services (Consulting)	FS Group	IT Specialist	Big Four (EY, Deloitte, PWC, KPMG)
	Compliance Control	ISSP	Sigma Software
	Active Audit Agency	XVand Corp.	EPAM Systems
	Iterasec	Underdefense	InfoPulse
		Exelegent	TUV-SUD

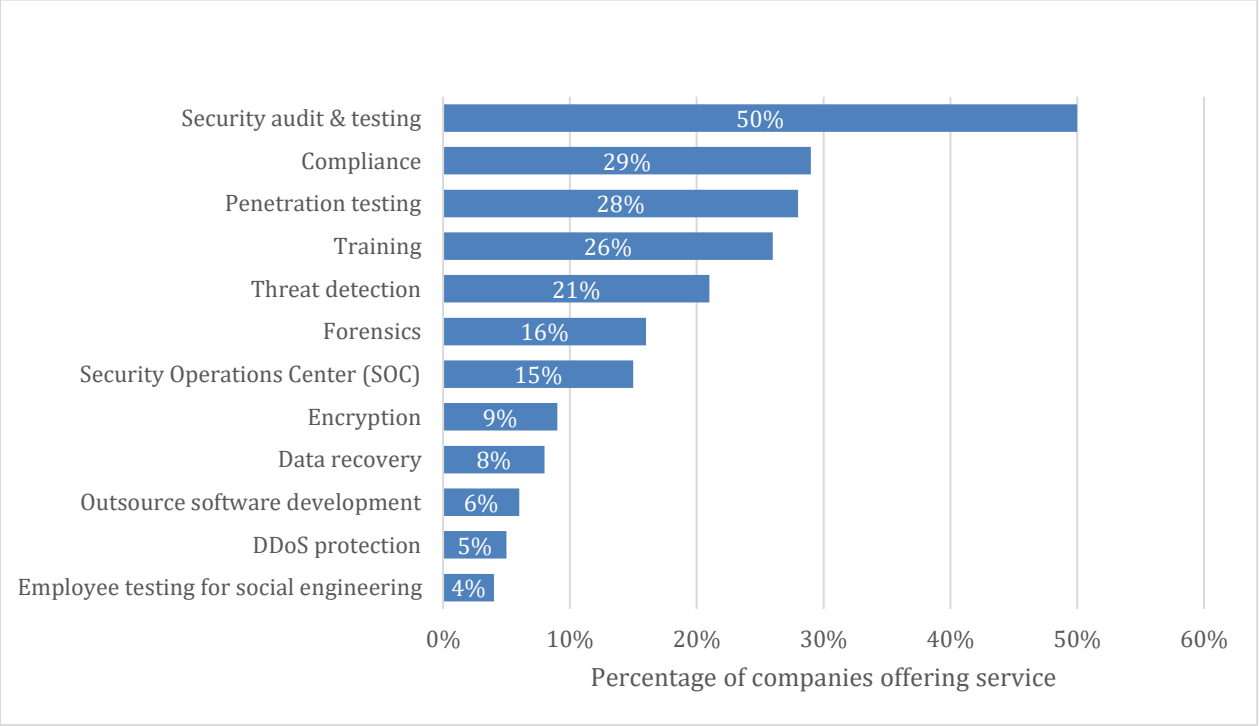
According to the market players interviewed, the Ukrainian cybersecurity market is at an early stage of development. This perception is confirmed by the types of products and services most prevalent

[5] In addition to businesses, private entrepreneurs in Ukraine provide cybersecurity services, including, for examples, pentests. However, individual private entrepreneurs are a very small part of the market—under the "private entrepreneur" designation, their annual income cannot exceed $35,526. For this reason, we have not included private entrepreneurs in this analysis.

and popular on the market, which primarily fall into the "Identify" bucket of the NIST Cyber Security Framework. While some Ukrainian firms do provide consulting services—including vulnerability assessments and penetration testing—for foreign clients, data on service exports are not available. In addition, gaining the trust of potential foreign clients is a challenge for Ukrainian cybersecurity consulting firms. One firm reported struggling to counter the perception that Ukraine is a center for cybercrime. This firm ultimately decided to pursue projects with the Government of Ukraine (GOU) that could subsequently serve to boost credibility for potential clients abroad.

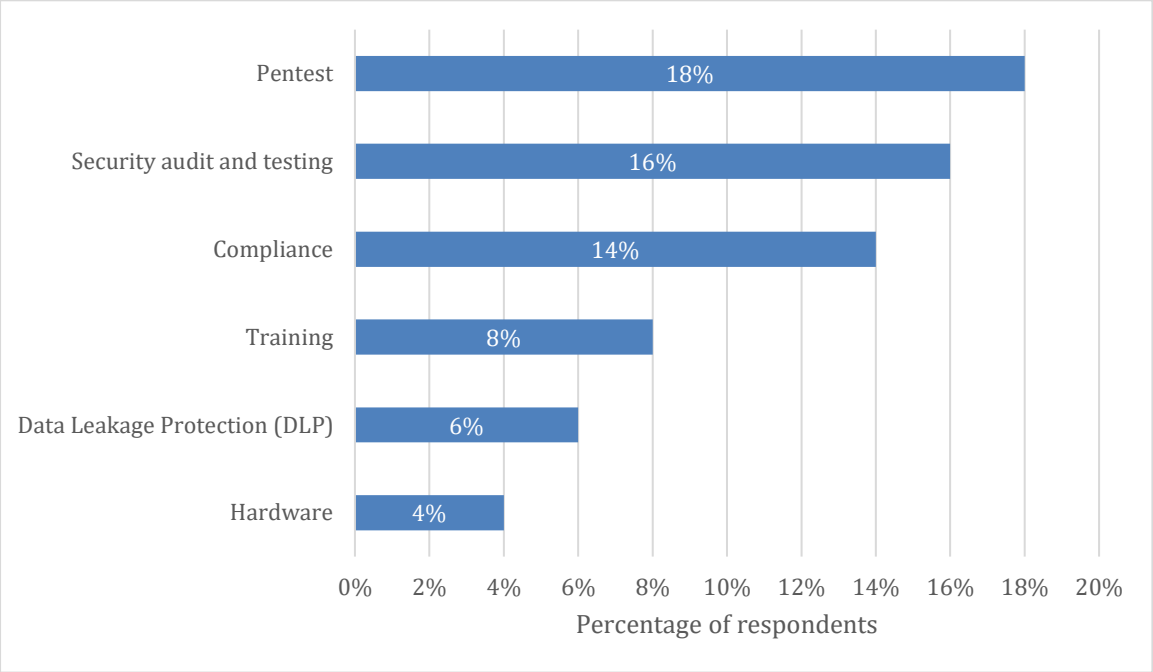
The main categories of cybersecurity services shown in Figure 2 are based on the analysis of marketing materials of the 72 Ukrainian cybersecurity firms.

FIGURE 2: PREVALENCE OF CYBERSECURITY SERVICES OFFERED ON THE MARKET



Twenty-two suppliers of cybersecurity products and services reported that their most popular three products/services lined up closely with the key services offered on the market (see Figure 3).

FIGURE 3: MOST POPULAR PRODUCTS AND SERVICES



FINDINGS FROM LARGE CYBERSECURITY CUSTOMERS

The survey results demonstrate that, in general, the larger operators perform more of the "Identify," "Detect," and "Recover" operations in-house. According to our survey of large companies devoting substantial resources to cybersecurity, 67% of respondents faced cybersecurity emergencies in the workplace in the past two years, and 33% of respondents experience cybersecurity incidents more than three times a month.[6] These firms often engage external cybersecurity consultants, and Figures 4, 5, and 6 show the breakdown between in-house functions and external services.

Question: "Is it possible to generalize and say that every firm involved in critical infrastructure should acquire three services (or products) right away?"

Answer: Yes.
1. Compromise assessment
2. Current vs. future state assessment with gap analysis, risk matrix, and roadmap
3. 24x7 Managed Detection and Response (MDR)/Security Operations Center (SOC)
—Ukrainian Cybersecurity Consultant

[6] Respondents were unwilling to share details on the severity and extent of the incidents.

FIGURE 4: PRODUCTS ACQUIRED EXTERNALLY BY MAJOR CONSUMERS

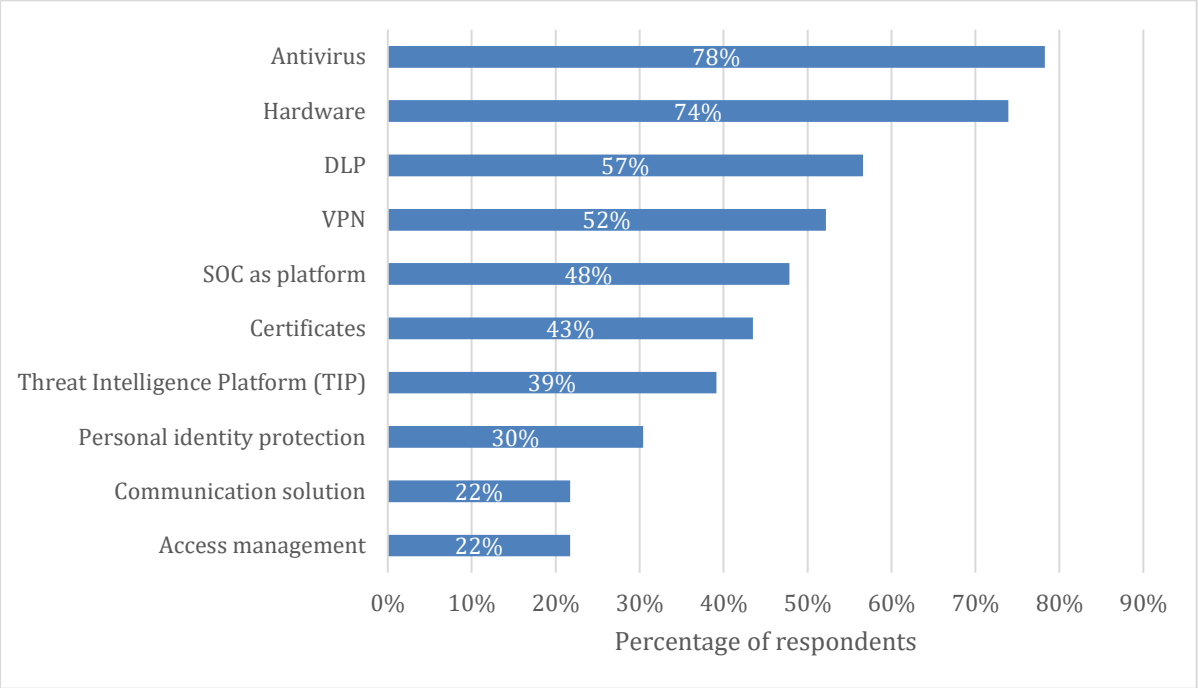


FIGURE 5: SERVICES ACQUIRED EXTERNALLY BY MAJOR CONSUMERS

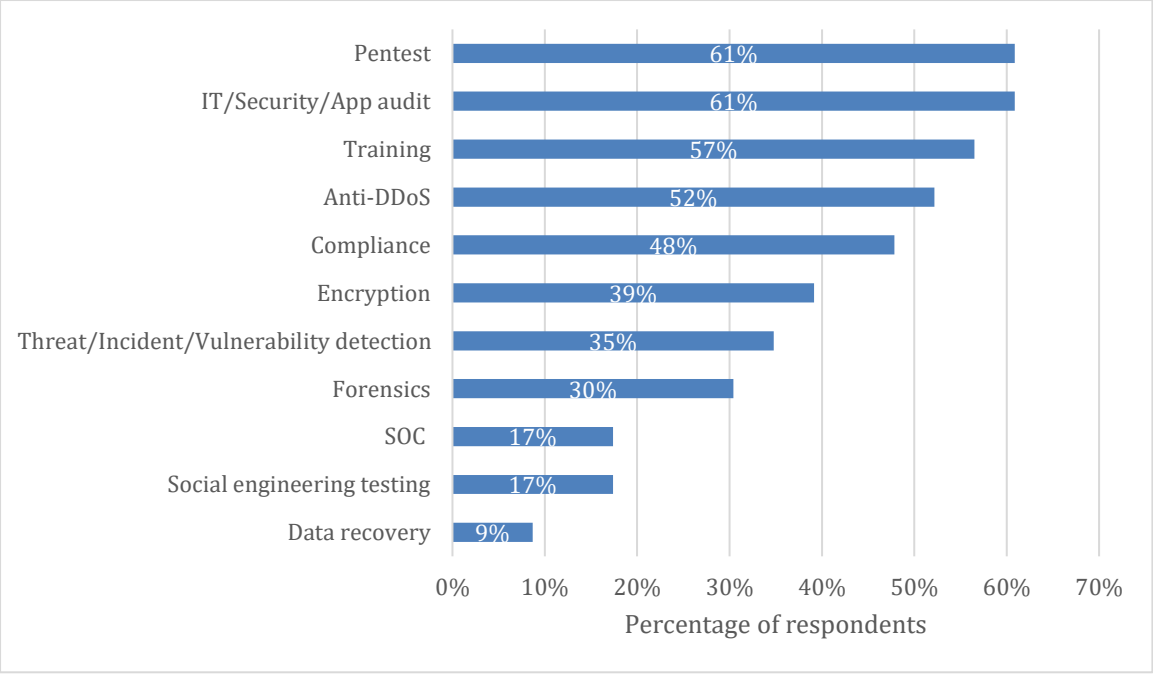
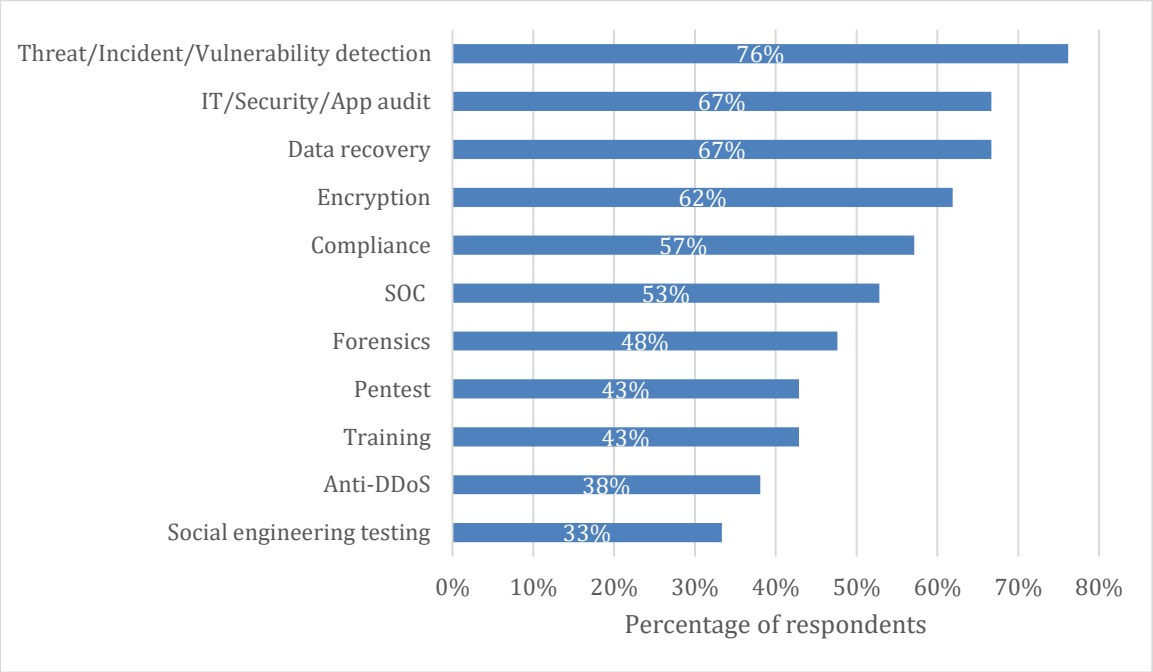


FIGURE 6: SERVICES PERFORMED IN-HOUSE BY MAJOR CONSUMERS



These findings suggest that major consumers often use in-house staff to perform day-to-day cybersecurity tasks and maintenance, including threat/incident/vulnerability detection, audits, and data recovery. Consumers more frequently turn to external firms and private entrepreneurs for more specialized cybersecurity tasks, like pen tests and anti-DDOS protections. Major consumers are also more likely to turn to external experts to train staff in cybersecurity.

IN-HOUSE CYBERSECURITY ACTIVITY & CYBER HYGIENE

Cybersecurity consulting firms stressed that there is no perimeter which cannot be breached and, as such, the key to cybersecurity defense is putting in place—and continuously updating—protections, constantly monitoring for breaches, and having plans to respond and recover data and/or restore operations quickly. While some products that automate monitoring functions (such as SOCs) are indeed expensive, especially for smaller users, much can be done in-house by CI operators by hardening the perimeter and maintaining a monitoring and updating regimen.

In the KIIs, the research team asked what was needed in Ukraine to stimulate market growth and improve cybersecurity. Besides regulation, key informants uniformly brought up cybersecurity education and emphasized the importance of preparing users (citizens and employees) and improving processes for better cybersecurity.

More than one person, unprompted, made the analogy to COVID-19: there is a series of steps you can take to reduce your risk of getting it (keep two meters away, wash your hands, don't let your guard down), but you also have to make sure everyone around you adheres to these guidelines.

Representative quotes are:

> "The most vulnerable link in the chain is human, not technology. This is why education awareness is a quick-win. A security awareness program is key to success."

> "90% of hacking is because of human factors."

> "First you establish an asset inventory database, implement hardening of environment (patches), and then you regularly monitor that you have the right versions. That's 85 percent of the threat." (This person cited the example of a three-page brochure prepared by the Australian government on "Strategies to Mitigate Cyber Security Incidents"[7] with 37 practical steps to take.)
>
> "There is a huge gap in the government sphere. Usually, they are using old software and have support systems that can't be protected."

While it is essential to put in place processes to detect and respond to cyberattacks, these systems cannot succeed if the staff tasked with implementing them do not practice strong cyber hygiene. Cyber hygiene is the combination of knowledge and practices at the individual level that decrease the risks of a cyber incident due to malware schemes, mishandling of data, or other vulnerabilities related to human behavior. Many market players mentioned cyber hygiene and awareness as a key aspect of strengthening the cybersecurity market in Ukraine. The more that decisionmakers—including government officials and CEOs—understand the threats posed by cyber incidents, the more likely they are to invest in cybersecurity products and services. Cyber hygiene also has implications for the cybersecurity workforce and, as such, resource allocations for cybersecurity, because improved cyber hygiene requires that entities hire more in-house cybersecurity support. In addition, the rapid shift to remote work has increased the need for robust cyber hygiene programs, as employees use both corporate and personal devices and network connections.

UKRAINIAN CYBERSECURITY MARKET SIZE

ESTIMATED CYBERSECURITY MARKET SIZE

Based on the four approaches outlined below, we estimate the size of the 2019 cybersecurity market in Ukraine to range from USD 84.8-126.8 million. This estimate accounts for in-house cybersecurity salaries. However, it does not consider the majority of defense and security service expenditures, for which data is not publicly available.

To develop this estimate, we have consolidated data from four sources: 1) analysis and adjustment of open-source data, 2) a detailed analysis of GOU tenders to corroborate the analysis of open-source data,[8] 3) 10 key informant interviews, and 4) a survey of 22 cybersecurity product and service providers:

1. The market size for goods and services sold on the Ukrainian market is approximately USD 110 million.
2. The public sector—not including defense and security end-users—was about USD 34 million, based on an analysis of ProZorro, the government's e-procurement system. Key informants estimated GOU spending makes up 50% of the entire market. Using these figures, we extrapolated a total market size of approximately USD 68 million.
3. Key informants estimated the product market was approximately USD 60 million, and that services made up between 15% and 30% of the market. Using the 15% figure, a conservative estimate of the total market is USD 70.6 million.

[7] "Strategies to Mitigate Cyber Security Incidents." Cyber.gov.au. Accessed March 15, 2021. https://www.cyber.gov.au/acsc/government/incident-mitigation-strategies.

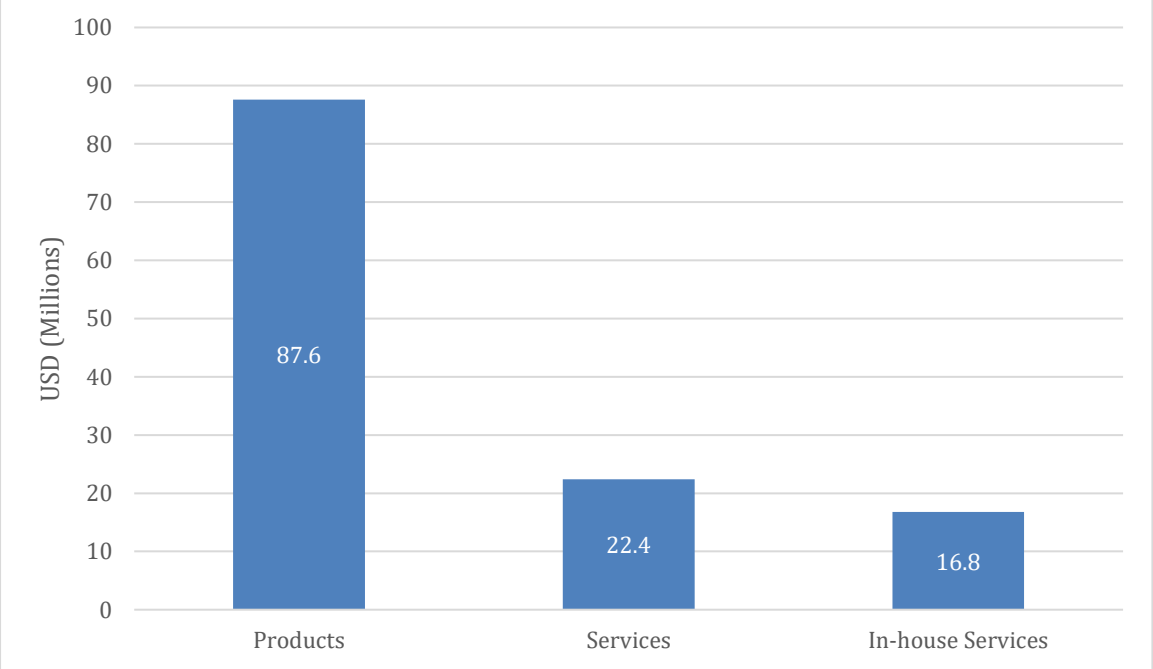
[8] In general, more information is available on government spending than on private-sector expenditures.

4. Half of the participants in the cybersecurity product/service provider survey estimated a market size of less than USD 100 million, and 37.5% estimated that it was between USD 100 and USD 250 million.

To each of these estimates, we added the estimated value of the salaries of in-house cybersecurity personnel (USD 16.8 million) (see pg. 19 for details on how the research team estimated this figure).

Thus, we established a market size ranging from USD 84.8 million to USD 126.8 million. Figure 7 shows the breakdown of this market by products, services, and in-house services for the high estimate (USD 126.8 million).

FIGURE 7: TOTAL MARKET SIZE 2019 (USD MILLION)

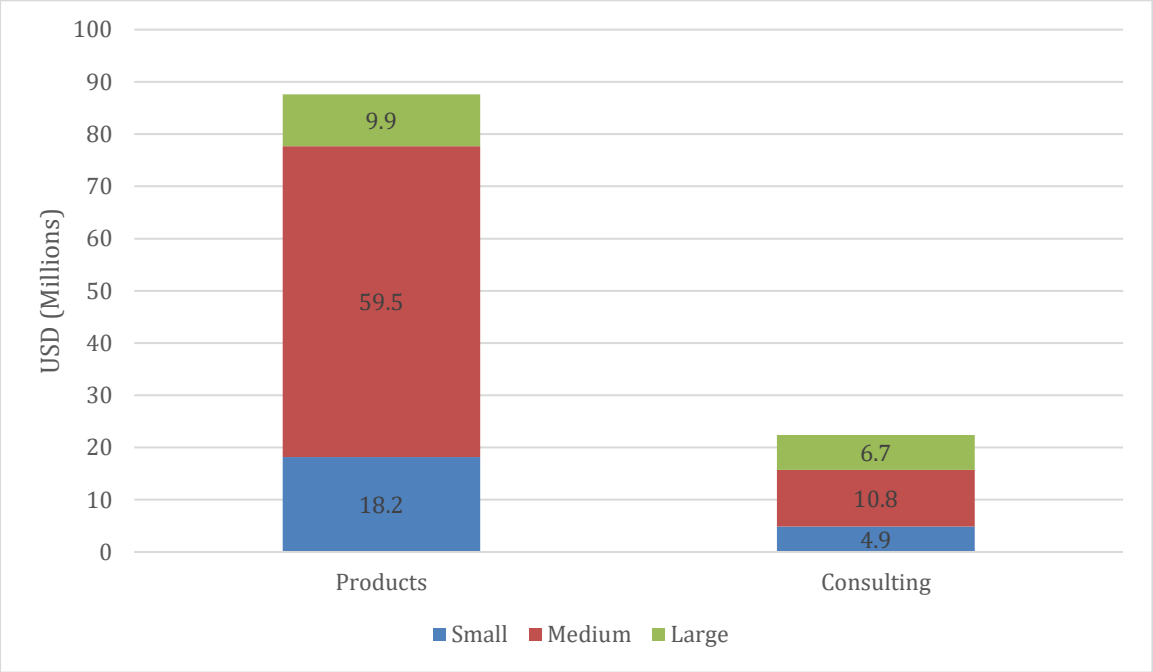


In the following sections, we present market size estimates by data source (adjusted open-source data, GOU procurement data, KIIs, and cybersecurity product/service provider surveys).

FINDINGS FROM ADJUSTED OPEN-SOURCE DATA

By taking publicly available data for the 72 cybersecurity firms analyzed and adjusting it to reflect the estimates of cybersecurity as a percentage of their total Ukrainian sales (see Annex 1), the research team estimated a market size (in 2019) of USD 87.6 million for cybersecurity products and USD 22.4 million for third-party consulting services, for a total of USD 110 million (see Figure 8).

FIGURE 8: ESTIMATED THIRD-PARTY GOODS & SERVICES (2019) (USD MILLION)[9]



Using this approach, the research team estimated that consulting services make up 20.4% of the market, which is at the lower end of the range estimated by key informants, who thought third-party consulting constituted 15-30% of the market for third-party goods and services, or up to USD 33 million.

FINDINGS FROM ANALYSIS OF GOU PUBLIC TENDERS

The public sector is a major portion of the cybersecurity market.[10] Accuracy in estimating the size of the public sector than the size of the private sector is greater because there is a fair amount of public data available about government tenders in Ukraine.

Before examining the tender data, the research team divided all public sector entities into three sectors:

1. State authorities – All official agencies, boards, commissions, committees, councils, departments, or other entities created by the legislative, judiciary, or executive branches at all levels of government.
2. State-owned enterprise (SOEs) – Business enterprises over which the state has significant control.[11]
3. Defense – Includes all military units, military educational institutions, and procurement departments in the Ministry of Defense. According to Article 3, Point 5.6 of the Law on Public Procurement as amended on 23.01.21, when a purchase is made for use in the defense sector, the ordering government entity has the right not to use the public tender

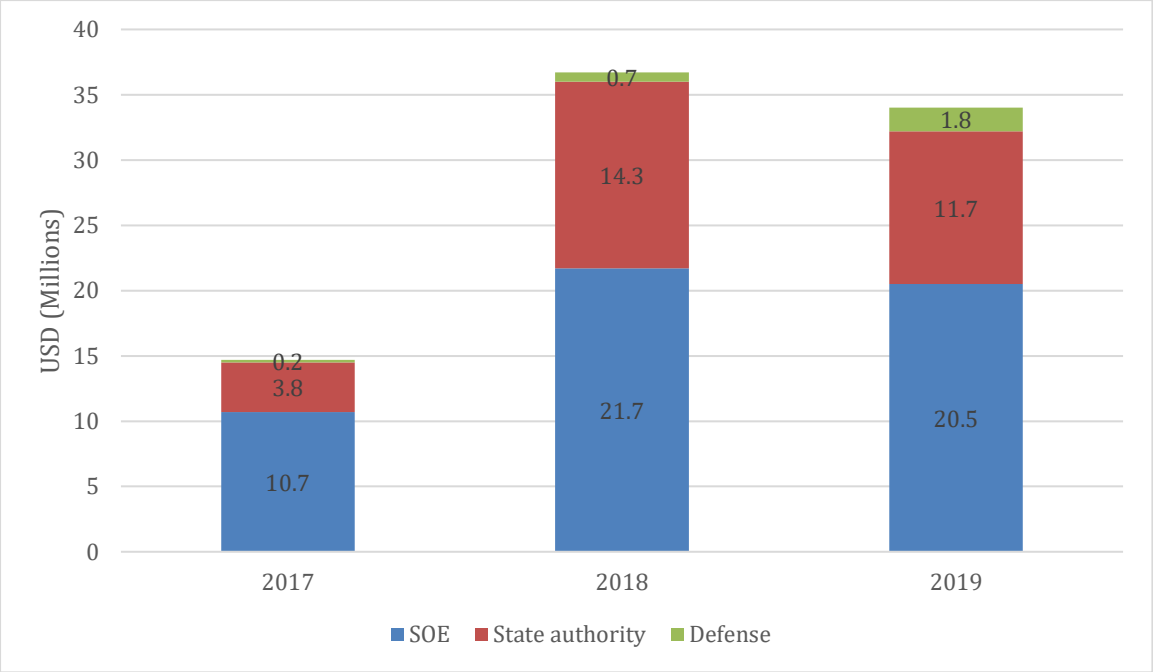
[9] The categories by the number of employees are as follows: small (fewer than 25 employees), medium (25-100 employees), and large (more than 100).
[10] While nearly no data are available on defense and security spending, the research team suspects that these sectors' spending on cybersecurity is substantial.
[11] The research team was unable to find tender information on Privatbank.

system, which explains why few public tenders for cybersecurity products and services with the military are available on ProZorro.

Information on public sector clients was found on clarity-project.info, an aggregator of Ukrainian government contract data from ProZorro, the government's e-procurement system. According to the information on ProZorro, 29 of the 72 cybersecurity suppliers provided their services to civilian state authorities, SOEs, and the defense sector. The total revenues from public procurement received by these companies from 2017 to 2019 amounted to USD 85.7 million across 2,052 contracts for 469 customers. Without the bulk of defense spending, yearly spending on cybersecurity tenders was USD 34 million in 2019, US 36.7 million in 2018, and USD 14.7 million in 2017. One well-placed key informant also estimated public sector spending to be about 50% of the market. This would then give a total market size of USD 68 million in 2019.

The following charts (Figures 9 – 12) show spending by sector, products vs. services, and major customers of ProZorro tenders.

FIGURE 9: PUBLIC TENDERS BY SECTOR (2017-19) (USD 85.7 MILLION)



While most public sector spending goes to products, consulting services consistently make up a substantial part of annual expenditures, averaging 32% of total spending over the past three years, as shown in Figure 10.

FIGURE 10: CONSULTING PRODUCTS – PUBLIC TENDERS (2017-19) (USD 85.7 MILLION)

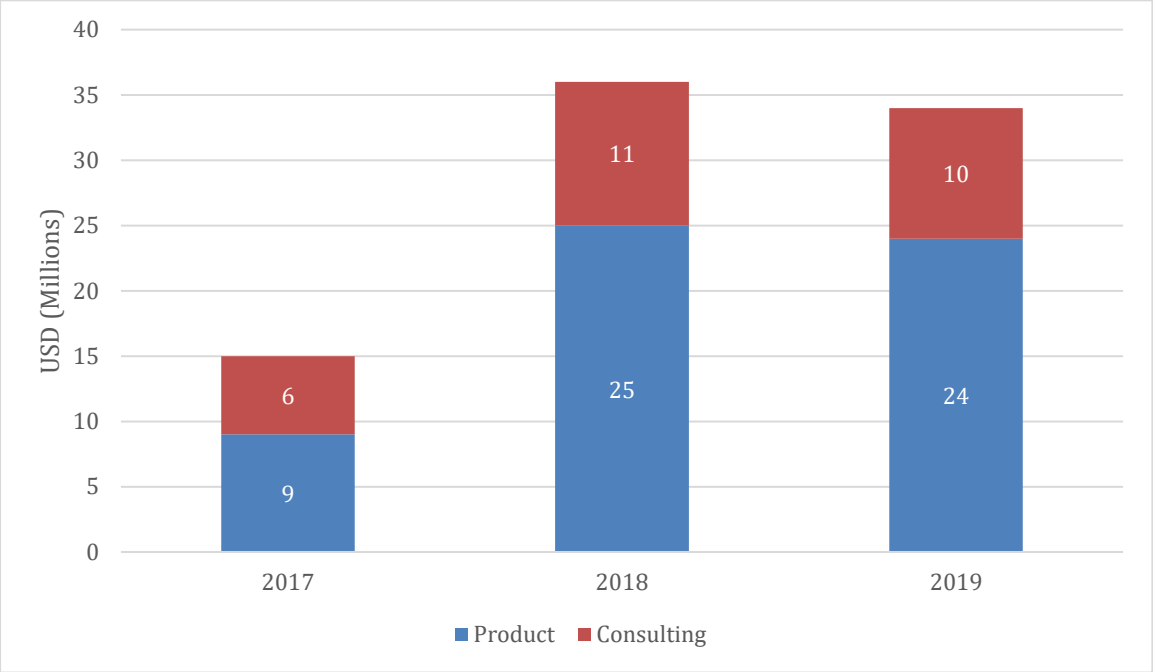
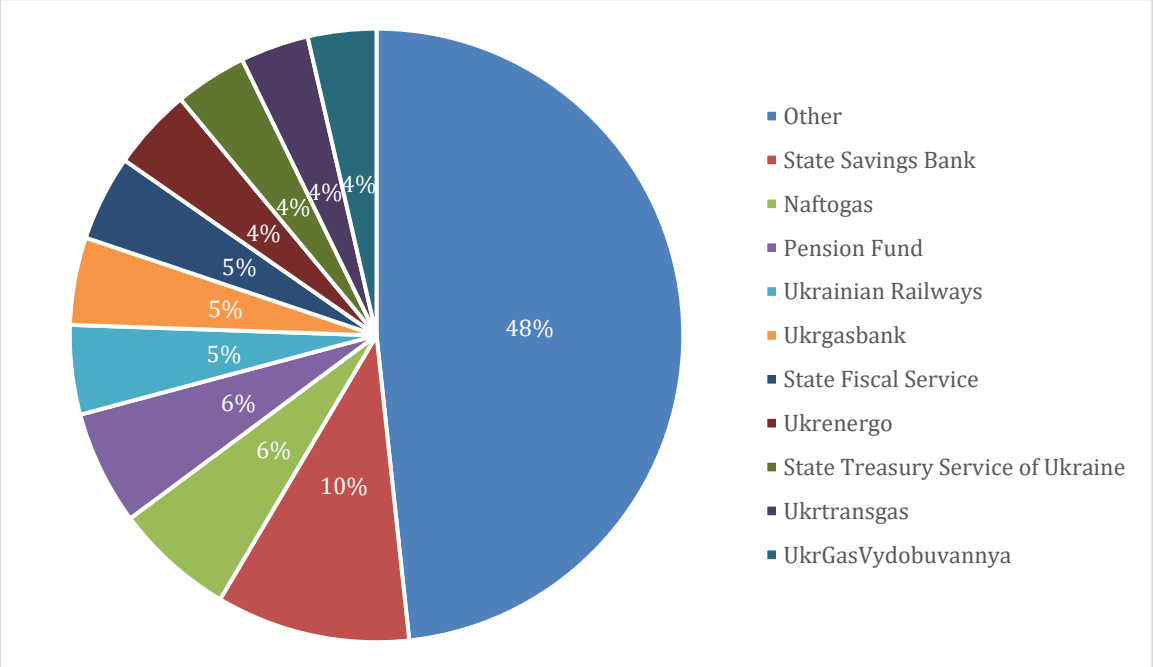


FIGURE 11: TOP 10 CUSTOMERS – PUBLIC TENDERS (2017-19) (BY MARKET SHARE)

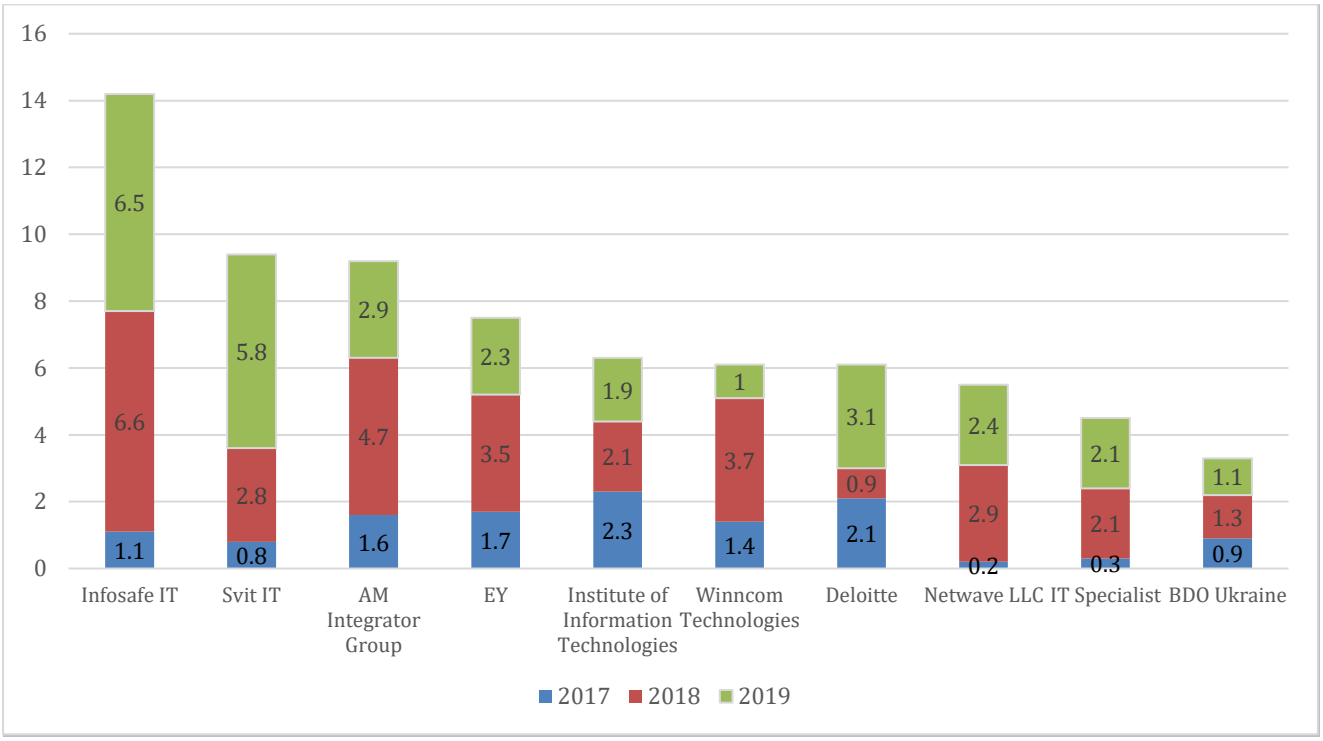


Please see Annex 2 for a breakdown of the top 10 customers in each of the public sectors (state authorities, SOEs, defense), as well as the major suppliers for each sector.

The chart below (Figure 12) shows the most successful bidders on public sector tenders by value of tender. While the firms are predominantly Ukrainian, the local affiliates of major international firms

such as EY and Deloitte play a substantial role in the consulting sector, where donor-financed cybersecurity projects drive much of the work.

FIGURE 12: LARGEST SUPPLIERS – PUBLIC TENDERS (2017-19) (USD 85.7 MILLION)



FINDINGS FROM KII ASSESSMENTS

Key informants were reluctant to estimate the size of the entire cybersecurity market. One major vendor estimated the value of hardware and software to be USD 60 million, which is not far off from the estimates given above. Of this amount, an estimated USD 8-10 million was for anti-virus software and USD 21-26 million for firewalls, leaving only about USD 24 million for more sophisticated cybersecurity software for threat monitoring. One respondent estimated that the GOU share of the cybersecurity market was about 50%. Various consulting firms estimate that the entire market is 15-30% services.

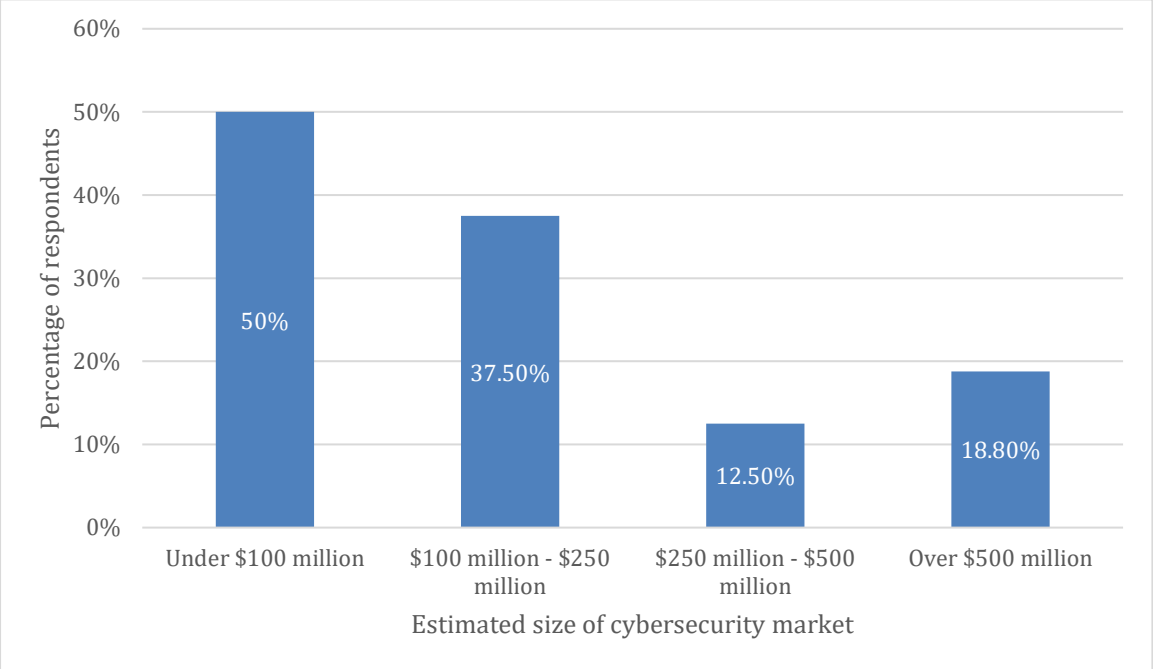
Taking USD 60 million for products, and assuming products make up 85% of the market, gives us a market size of USD 70.6 million.

Key informants mentioned that figures for current hardware sales may not be indicative of cybersecurity spending in the future. One key informant expects the budget allocation split between hardware and software to go from about 50-50 now to 20-80 in the coming years. Hardware is often more expensive and therefore more attractive for those interested in profiting from corruption. It's also important to note that in many organizations hardware budgets are larger than software budgets for both public and private sector entities. A shift in the perceived value of licensed software and subscription services will likely shift this balance relatively rapidly.

FINDINGS FROM PRODUCT AND SERVICE PROVIDER SURVEY

Half of the 22 survey respondents estimated that the market could be as large as USD 100 million, and the second largest group (37.5%) estimated it to be between USD 100 and USD 250 million (see Figure 13). Estimates larger than USD 250 million may indeed be an assessment of third-party goods and services on the market; they may, however, simply indicate that some respondents included the work of large IT outsourcing on cybersecurity projects or the entire market for cloud storage and services.

FIGURE 13: MARKET SIZE ESTIMATES (SURVEY)



FINDINGS FROM ASSESSMENT OF SPENDING ON IN-HOUSE CYBERSECURITY PERSONNEL

Estimates of the number of cybersecurity professionals at third-party consulting firms in Ukraine ranged from 350 to 500 people. One expert estimated that three to five times as many cybersecurity professionals work in-house at government and private entities. If we assume that means 2,000 employees, at an average 2019 annual wage of USD 8,400[12] (the rate for junior employees), then the public and private sector spent approximately USD 16.8 million on in-house cybersecurity. The research team took the 2019 salary of junior software engineers, reasoning that a large portion of in-house cybersecurity employees was in the public sector, where salaries are low. The salary information is from the site dou.ua, an online clearinghouse for IT-industry analytics, research, and employment and salary information.

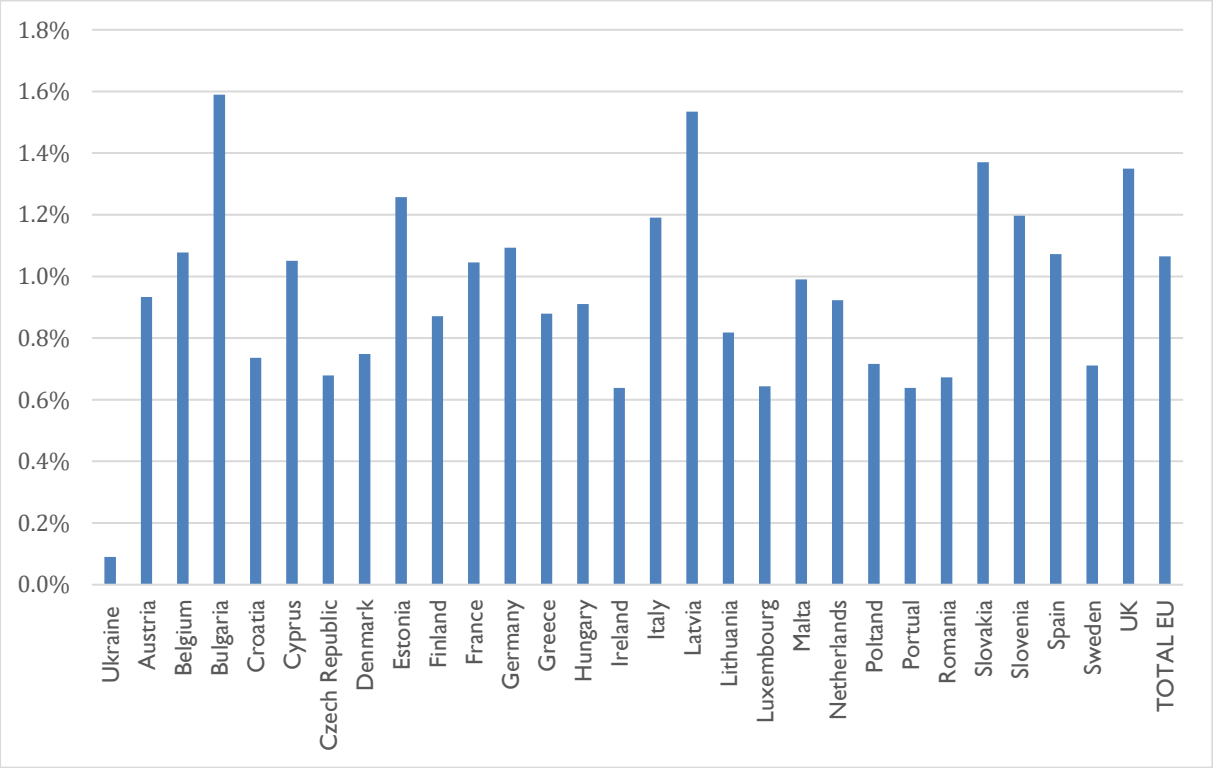
GAP: DEMAND VS. NEED

While the assessment has produced a fairly broad estimate of the size of Ukraine's cybersecurity market, the fact remains that the market is minuscule compared to nearly all European national

[12] "Salaries of Ukrainian Engineers – Winter 2021." DOU. Accessed March 15, 2021. https://dou.ua/lenta/articles/salary-report-devs-winter-2021/.

markets. In 2019, Ukrainian GDP was USD 153.78 billion,[13] and the size of the Ukrainian cybersecurity market was USD 84.8 million to USD 126.8 million, which is 0.055% to 0.082% of GDP. According to a 2018 study of the 2016 EU cybersecurity market carried out by PwC and LSEC,[14] the average size of the cybersecurity market in EU countries was 1.1% of GDP (see Figure 14). Even the lowest-ranking countries (Ireland, Luxembourg, and Portugal) had markets that were 0.6% of GDP. Thus, for Ukraine to rank with the lowest spenders on cybersecurity in the EU, its market size would need to grow to USD 923 million; to reach the EU average, the country would need to spend USD 1.69 billion.

FIGURE 14: CYBERSPENDING AS PERCENTAGE OF GDP



Partial corroboration of this gap comes from estimates put forth in the KIIs. Key informants reported that the public sector only covers 20% to 25% of its cybersecurity needs and that the government only covers between 20% to 50% of its cybersecurity staffing needs.

[13] The World Bank, "GDP (Current US$) – Ukraine."
[14] European Commission, *Cybersecurity Industry Market Analysis – CIMA,* p. 84.

MARKET GROWTH CONSTRAINTS AND RECOMMENDATIONS

OVERALL MARKET

1. Insufficient Legal and Regulatory Framework

Key informants indicated that current laws and regulations do not require companies or public entities to proactively address gaps in their cybersecurity, and emphasized that an improved legal and regulatory framework based on international best practices and standards would drive growth in the cybersecurity market by simultaneously requiring organizations to make investments and guiding those decisions through clear frameworks and policies. And while providers of cybersecurity products and services see regulation as necessary for market growth, some caution that regulation is not a panacea because regulation can be circumvented through measures that demonstrate compliance on paper only. In this regard, a system of reliable and transparent third-party audits would bring credibility to compliance and further support wise decision-making regarding cybersecurity investments.

The Activity should also consult with and learn from the past experience of other Ukrainian cybersecurity stakeholders when recommending changes to the legal and regulatory framework. As part of its support for improved cybersecurity regulation the Activity should consult with the National Bank of Ukraine (NBU) to better understand recent experience with cybersecurity regulation in the financial sector. Interviewees indicated that the NBU pursued an approach several years ago which was not widely viewed as a success. In 2012, the NBU issued an obligation for all banks in Ukraine to implement an information security management system (ISMS). Interviewees noted that many of the banks met the minimum obligation without having to make serious changes to their systems. However, now experts point to the financial sector as being ahead of other sectors in terms of cybersecurity, especially as related to threat intelligence sharing.

2. Limited Awareness of Cybersecurity Risks and Solutions among CI Operators

Most interviewees believed that while organizational leaders (i.e. decision makers) are generally aware of the risks posed by cyberattacks, they did not understand how attacks or incidents could specifically affect critical functions, operations, services, or organizational reputation. One interviewee noted a tendency not to act until after an attack. In addition, decision makers often fail to grasp the financial cost of a cybersecurity attack and, therefore, regard cybersecurity as a pure cost center. A number of interviewees said most operators associate cybersecurity only with IT, resulting in dangerous neglect of operations technology (OT).

When asked what specifically could be done to increase cybersecurity market activity, senior staff repeatedly came back to one concept: education and awareness. Employees need training on cyber hygiene practices; CISOs and CIOs must understand how to improve cybersecurity and justify cybersecurity investments to management; and CEOs must understand the financial risks of failing to improve cybersecurity.

Participation in industry-specific fora could help raise awareness of cybersecurity issues and facilitate the exchange of information about threats and solutions (see Table 3). While many such events have been postponed until further notice due to the COVID-19 pandemic, some will continue using an online format.

TABLE 3: MAJOR CYBERSECURITY EVENTS

NAME	DESCRIPTION	ORGANIZERS
UISGCON	Gathers hundreds of Ukrainian and international experts in information security in Kyiv to discuss the industry's most acute problems. Website: http://uisgcon.org/	Ukrainian Information Security Group (UISG), an NGO
NoNameCon	100% community-built practical cybersecurity conference in Kyiv, Ukraine. Website: https://nonamecon.org/	UISGCON, OWASP Kyiv, Securit13, NoNamePodcast
McAfee Cybersecurity Forum	Looks at the most recent trends in cyber threats in Ukraine and around the world, as well as the most recent approaches and technologies to detect and prevent complex targeted attacks and 0-day threats. Website: https://bakotech.com/events/McAfeeFinForum2020/	McAfee, Bakotech
InfoSec MeetUp, InfoSec Cruise	Devoted to the internal security of organizations, the fight against insider threats, and methods of controlling users who put companies at risk.	Bakotech, Netwrix, ObserveIT, One Identity
Smart Security Day	Dedicated to the most productive UTM devices, which reflected the largest number of attacks in the NSSLabs test environment in 2019 during testing for next-generation firewalls. Website: https://bakotech.com/events/SmartSecurityDay	Bakotech, WatchGuard
OWASP Ukraine	Ukrainian Application Security conference held under the aegis of OWASP Lviv, Kyiv, Dnipro, and Kharkiv chapters. Website: https://owaspukraine.org/?ref=infosec-conferences.com	OWASP
DC8044: BLACKOUT	Free hacking and networking event Website: https://dc8044.com/	DEFCON Kyiv community
BSides Kyiv	Community-driven framework for building events for and by information security community members.	R0-Crew, OWASP Odessa, OWASP Lviv, and UISG
UA.SC	A platform where cybersecurity experts share experience and solutions for building corporate IT security. Website: https://uasc.com.ua/	Integrity Vision

3. Limited Resources for Cybersecurity Expenditures

Both product and service providers said that more comprehensive cybersecurity programs were often financially out of reach for enterprises that needed them. A specific goal might be to make SOCs—which are key to detecting threats—accessible and affordable to smaller players, potentially by providing financing to reliable outsourced SOCs.

One major cybersecurity product provider in Ukraine has a financing vehicle for its customers to purchase its products in the North American market.[15] This might be a structure worth investigating for replication in Ukraine.

CYBERSECURITY FIRMS

1. Market Size and Growth

The Activity cannot expect a significant number of Ukrainian cybersecurity firms to grow substantially unless the market grows proportionally. Leaving aside the market size issues highlighted above, growth expectations for the firms surveyed varied. Some smaller players expected annual growth of anywhere between 0% and 30%, and they frequently complained of price competition and lack of demand as constraints to growth. Larger players offering consulting services, who often have foreign customers, reported attempts to focus on the Ukrainian market were frustrating. They predicted limited growth without stronger regulation and greater awareness of cyber risks.

2. Lack of Qualified Professionals

Sixty-nine percent of survey respondents and all key informants noted a shortage of highly qualified cybersecurity specialists. Factors contributing to the shortage include the emigration of specialists and competitive career opportunities in Ukrainian IT outsourcing companies. In addition, experts observed that it takes even a highly qualified graduate at least one year to learn the ropes and perform at a level consistent with his or her salary.

3. Insufficient Financing Options

Information on investment in the industry is limited, largely because most companies do not publish information about investment terms. In the survey interviews, most respondents said that an initial investment of up to $300,000 would be sufficient to start a company (i.e., hire and equip up to 10 employees of average qualification and cover the first year's expenses). While some surveyed cited financing as a problem for starting a business, a majority cited the difficulty in finding customers and qualified employees.

For an investment to be effective, a firm would need to hire and retain a sufficient number of qualified staff for at least two years—one year to win business and a second to execute new contracts. Successful investments require adequate demand for a company's services. As neither of these is guaranteed in today's cybersecurity market in Ukraine, providing financing to cybersecurity startups may not alone address the key issues.

PRIORITY NEXT STEPS

Improving the cybersecurity market in Ukraine is a complex endeavor that will require support from multiple stakeholders across the public and private sector. In this section, we highlight the priority next steps for strengthening Ukraine's cybersecurity market and indicate where the Activity can support other stakeholders.

MARKET FUNDAMENTALS

1. CI Asset Inventory and Prioritization

[15] https://www.cisco.com/c/en/us/buy/payment-solutions.html

The GOU has embarked on an important initiative to inventory all of its CI assets. This critical, lengthy, and highly complex process will enable the GOU to assess the landscape of CI assets as a basis for cybersecurity prioritization and risk management. Ultimately, this approach will facilitate more strategic decision making for cybersecurity solutions in the public sector, which in turn will serve as a catalyst for market growth. In addition, this process will encourage greater coordination between the GOU and CI assets, improving understanding of cybersecurity threats. This better understanding of threats is an important market dynamic because it allows organizations to seek cybersecurity solutions that can mitigate those threats. This can have a longer-term market impact on the cybersecurity sector.

The Activity is supporting the GOU to develop its registry of CI assets by assisting in the technical development and implementation of the registry, development of policies and practices, and training of users.

INCREASED DEMAND AND CYBERSECURITY INVESTMENT

1. Appropriate Regulations to Foster Market Growth

Efforts under Component 1 (Enabling Environment) of the Activity to improve the regulatory environment for cybersecurity will help increase demand for cybersecurity goods and services by applying reasonable and transparent regulations based on international best practices. This must also be supported by efforts to provide entities with resources to comply with rather than circumvent regulations (e.g. guides to implementation, information on best practices, affordable consulting services, etc.). The NBU example cited earlier can provide valuable lessons learned to improve regulation enforcement in the future.

2. Increased Awareness of Cyber Risks among CI Operators and GOU Stakeholders

The Incident Preparedness Plan developed by the Activity focuses on increasing awareness of vulnerabilities at the CI operator level through cybersecurity diagnostics in selected entities and development of a Cyber Maturity Model (CMM) for widespread use. These tools result in improvement plans which CI operators can implement to improve their overall cybersecurity posture. The Plan further builds national preparedness by increasing the exchange of threat intelligence between stakeholders—in both the private and public sector—for improved systemic resilience. These combined approaches will result in a greater awareness of threats at the organizational level, as well as common vulnerabilities at the ecosystem level, giving decision makers more information about where to invest limited resources based on priorities. This is a significant opportunity for private sector engagement and therefore market growth. The Activity can increase this awareness in a number of ways:

a. Ensure private sector engagement in threat intelligence sharing—as active participants to strengthen the overall ecosystem, but also as service providers. In this way, companies offering relevant services or products can be seen as viable options for addressing specific challenges. Also, effective threat intelligence is an opportunity for public-private partnerships, where local private providers can engage in the provision of open source threat intelligence, combined with value-added analysis for improved detection and response as part of a system supported by the public sector cybersecurity stakeholders.
b. Accelerate and expand plans for the CMM to motivate decisionmakers—including government officials and CI managers—to invest in cybersecurity by showing the potential financial losses for cyberattacks and the opportunities related to improved cyber maturity.

For example, potential partners, customers, and investors will have greater confidence in Ukrainian entities that can provide proof points related to their cyber maturity.

c. Adapt the CMM into a simplified diagnostic tool for smaller enterprises. This simple modification, perhaps in partnership with organizations like the Global Cyber Alliance (which offers a cyber toolkit for SMEs), could significantly impact market demand for cybersecurity services and products targeted at this segment.

In addition to these steps that will increase cybersecurity knowledge and understanding, the Activity will collaborate closely with government, private sector, and donor counterparts to support additional awareness efforts. For example, the Activity is currently planning a cyber hygiene training for GOU employees across multiple ministries. Working closely with Chief Digital Transformation Officers (CDTOs), the Activity will conduct trainings that increase overall GOU awareness of cyber threats and will ultimately create more demand for cybersecurity products and services. The Activity will also coordinate closely with other donors working on cyber hygiene initiatives in Ukraine, including the Organization for Security and Cooperation in Europe, CRDF Global, and the International Federation for Electoral Services.

INCREASED SUPPLY AND IMPROVED QUALITY OF CYBER SMBs

1. Workforce Development at University and Professional Levels

In order for companies—and by extension, the cybersecurity sector—to grow and innovate, Ukraine will need a robust workforce of cybersecurity specialists. This is especially critical for the growth of cybersecurity SMBs. The Activity addresses this priority through its Workforce Development Plan and tasks under Component Two, specifically the Cybersecurity Higher Education Program and Upskilling Professionals initiative.

2. Investigate Financing Vehicles for Cybersecurity Products and Services

Given the low demand and small market for cybersecurity services and products at present, and the long lead time for developing a financing vehicle, the Activity should investigate options to create a vehicle or establish partnerships to invest in cybersecurity firms (e.g., start-up grants and working capital). Over time, increasing demand will justify further investment from a range of sources. The Activity is currently writing an Investment Strategy that will investigate and propose appropriate vehicles and partnerships to stimulate investment in Ukraine's cybersecurity sector.

3. Focus on Cybersecurity SMB Capacity Building

While the Activity will begin developing financing vehicles to encourage investment in the cybersecurity sector, SMBs working on cybersecurity might benefit from other forms of support, like business training. Even though their solutions might be just as strong—and, in some cases, less expensive—Ukraine's cybersecurity SMBs often cannot compete with international firms due to underdeveloped business and marketing skills. In addition to advising on generic marketing and sales materials (including content marketing and the development of open-source tools), this support should help SMBs distribute information about threats and responses. The Activity will support SMBs to build these skills through its SMB Accelerator and SMB Mentorship programs under Component Three. Additionally, the Activity's Exchange Platform will help Ukrainian cybersecurity firms market their offerings to new potential customers in Ukraine and internationally.

4. Engage the Cybersecurity Community and Improve Access to Market Information

The Activity proposes strengthening the cybersecurity community in Ukraine to give a voice and increased visibility to professionals as well as businesses. Through the Center for Cybersecurity Innovation (CCI), the community will identify priorities for reform, capacity building, and market growth, as well as network and explore partnerships. The proposed MELISSA Market Information Exchange Platform will provide high quality market information, connect providers with customers, and ensure informed and strategic cybersecurity purchase decisions, particularly on the part of resource-constrained public sector entities and CI operators.

ANNEX 1. INFORMATION SOURCES AND METHODOLOGY

1. 23 major cybersecurity consumer survey interviews

SECTOR	NO. OF COMPANIES	POSITION(S) OF THOSE INTERVIEWED
Finance and Banks	3	Director of Information Security, Head of Information Security Department
Manufacturing	1	CIO
Energy	1	CIO
Payment Processing	1	CIO
Product Development	4	Chief Technology Officer (CTO), Chief Solution Architect, Security Engineer, Quality Assurance (QA) Automation Lead
Telecommunications	2	ICT Security Analyst, Head of Information Security & Infrastructure Development Department
Healthcare	3	CIO
Outsource Services	1	Senior Cloud Security Architect
Retail	3	Head of Information Security and Technical Security of Retail Sales, Head of Information Security Department, Head of Cybersecurity Department
Government	4	Head of IT Audit, Information Security, Head of the Training Center, Head of Information Security Department, Head of ICT Department

2. 22 Product and Service Providers survey interviews[16]

SECTOR	NO. OF COMPANIES	POSITION(S) OF THOSE INTERVIEWED
Consulting	16	Owner, Co-founder, Director, CEO, Business Development Director, Operations Director, Senior Security Consultant, Cybersecurity specialist, Principal Security Consultant, Cyber Security Consultant, and IT Security Consultant.
Product	5	Co-Owner, CEO, Director, IT Specialist & Head of Government Business, Head of IT Security Solutions Department, Director of the Department.

3. Methodology of Adjusting Open-Source Revenue Data

Based on research using databases, websites, and interviews, the research team estimated 72 companies supply cybersecurity products and consulting services in Ukraine.

Revenue figures for these companies came from public annual reports, press releases, news articles, as well as from company profiles on YouControl, a website that provides information on balance

[16] The 22nd interview in this group was an IT Security Consultant, who was chosen as an independent cybersecurity expert without affiliations to major market players.

sheets and profit and loss (P&L) figures for Ukrainian businesses.[17] Out of the 72 companies, revenue figures for 2019 were available for 45 companies. For the 10 companies that provide multiple services but focus mainly on cybersecurity and the 23 companies with revenue of less than $1 million, the research team made no adjustments. For the remaining 12 companies with multiple service lines and substantial non-cyber activity, such as the large international consulting and hardware/software vendors (who often had classical IT operations), the team made the following adjustments:

- For cybersecurity consulting firms – Based on breakdowns of services in company reports as well as on interview responses, 5% of total revenues.
- For hardware/software manufacturers and integrators – 10 to 50% of total revenue based on public information that the company has posted about its cybersecurity activity.

The research team then divided the companies into the categories of small, medium, and large by the numbers of employees. For the 27 companies without 2019 revenue data, these companies earned the average revenue of the companies for which there were revenue figures or estimates in the same category.

To summarize, the estimation of 2019 market size was based on the following (Table 4):

TABLE 4: COMPANIES AND REVENUE METHODOLOGY

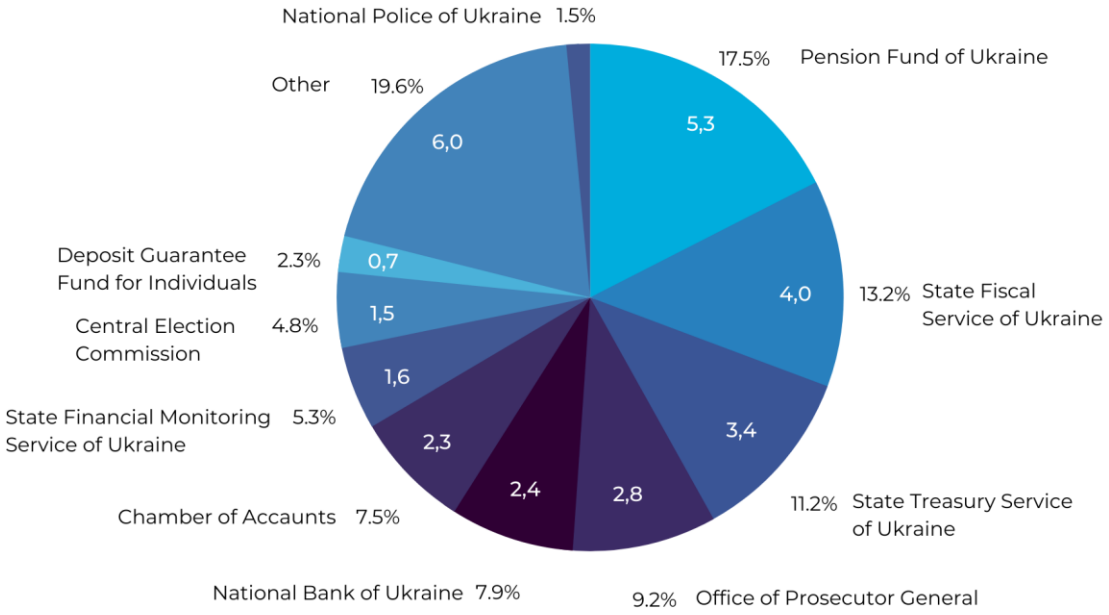
REVENUE INFORMATION FOR COMPANIES	NUMBER OF COMPANIES
Companies with public revenue data (unadjusted)	33
Companies based on public revenue data but adjusted	12
Companies with no public revenue data; revenues extrapolated based on size category	27
TOTAL	72

The research team cross-checked the revenue estimates with the figures from 2019 public sector tenders, and for those seven companies whose tenders were greater than the revenue estimates, it took the higher figure from the tenders. This was a total correction of USD 8.14 million.

[17] The values were converted from UAH into USD using the following annual average exchange rates published by the National Bank of Ukraine: 1 USD equaled 25.55 UAH in 2016, 26.59 UAH in 2017, 27.20 UAH in 2018 and in 25.85 UAH in 2019.

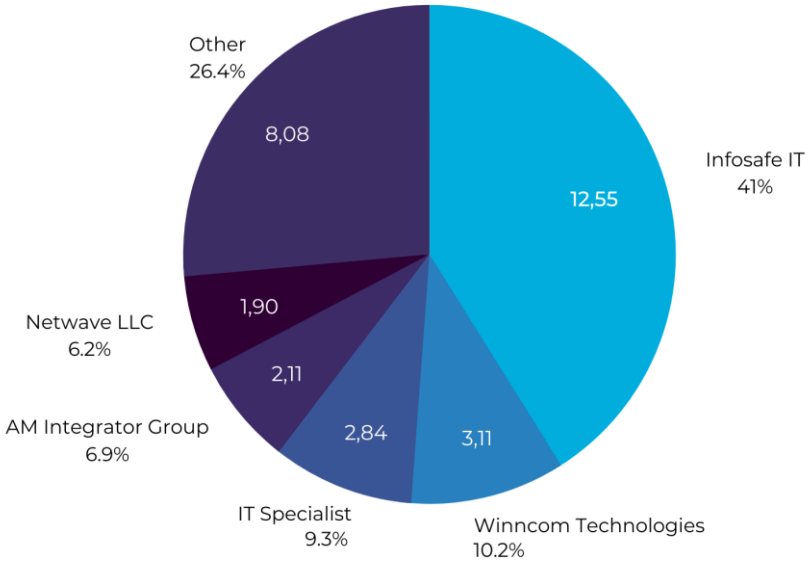
ANNEX 2. PUBLIC SECTOR CYBERSECURITY TENDERS BY SECTOR

FIGURE 15: CUSTOMERS OF PUBLIC TENDERS—STATE AUTHORITIES (2017-19) (USD 30.6 M)



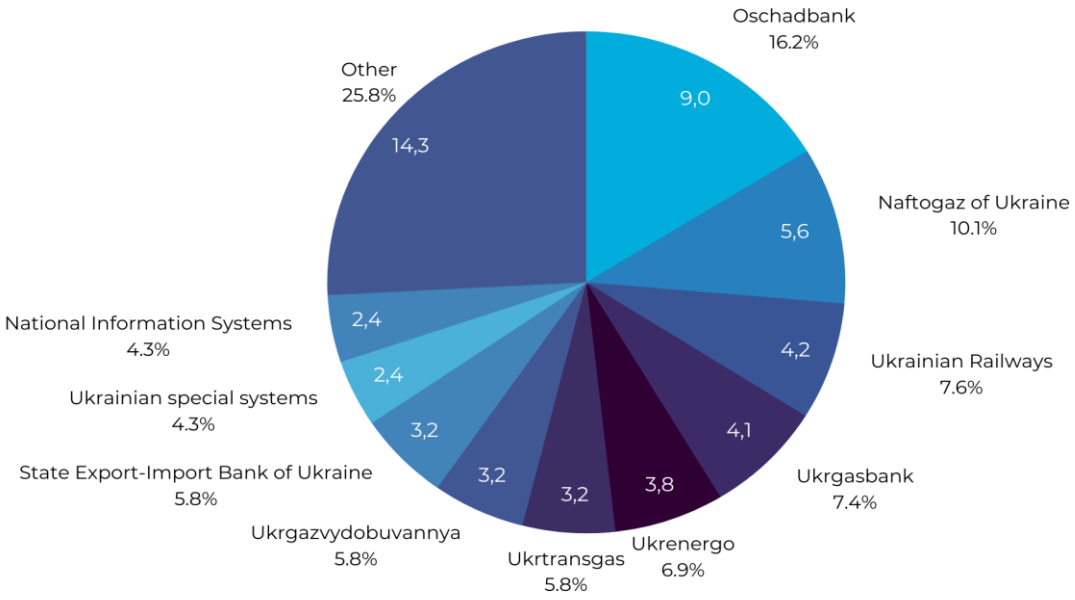
Note: Other includes 178 additional state authorities.

FIGURE 16: MAJOR SUPPLIERS TO STATE AUTHORITIES—PUBLIC TENDERS (2017-19)



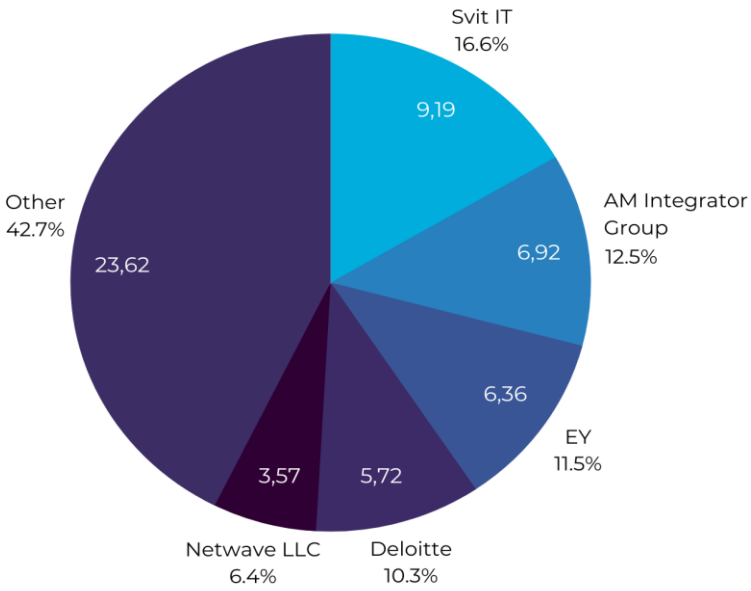
Note: Other includes 20 additional cybersecurity providers.

FIGURE 17: SOE CUSTOMERS OF PUBLIC TENDERS (2017-2019) (USD 55.4 M)



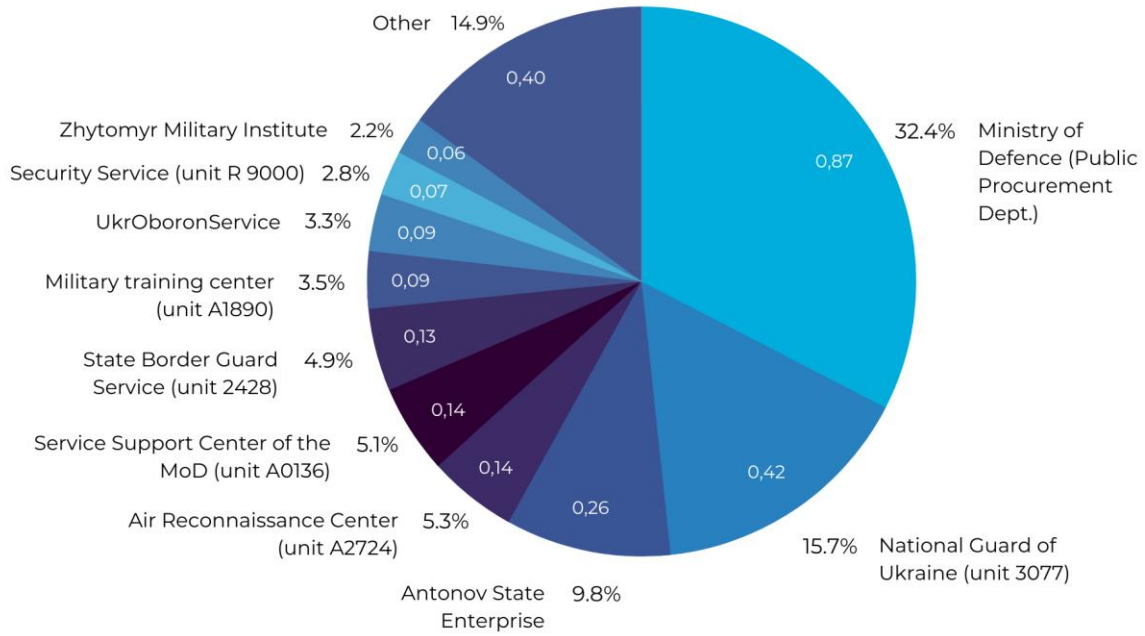
Note: Other includes 236 additional SOEs.

FIGURE 18: MAJOR SUPPLIERS TO SOE—PUBLIC TENDERS (2017-19)



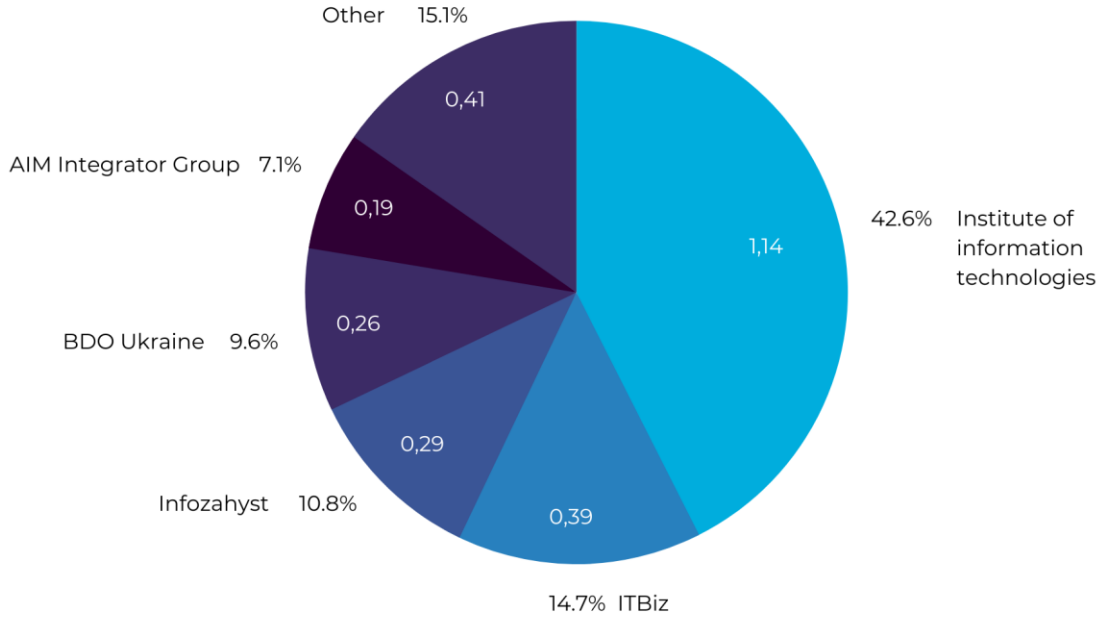
Note: Other includes 22 additional cybersecurity providers.

FIGURE 19: DEFENSE BENEFICIARIES – PUBLIC TENDERS (2017-19) (USD 2.6 M)



Note: Other includes 26 additional defense agencies.

FIGURE 20: MAJOR SUPPLIERS TO DEFENSE—PUBLIC TENDERS (2017-19)



Note: Other includes 7 additional cybersecurity providers.